Haekka

Lesson 1 | Introduction to PCI

Updated 2020-09-30

PCI, or often PCI DSS (Payment Card Industry Data Security Standard), is an industry-led security standard to create a baseline for the security of financial, specifically cardholder, data. PCI applies, as a requirement, to all companies that process card payments and all companies that *store, process, or transmit cardholder data and/or sensitive authentication data*.

PCI Data

PCI is concerned with two types of data - 1) cardholder data (CHD) and 2) sensitive authentication data. There are key distinctions in how these types of data need to be handled. Cardholder data can be stored but sensitive authentication data cannot be stored.

Cardholder data (CHD)

- Primary account number (PAN)*
- Cardholder name
- Expiration date
- Service code

* Primary account number (PAN) is the "defining factor for cardholder data".

Sensitive authentication data

- Full track data (magnetic stripe or equivalent)
- CAV2/CVC2/CVV2/CID
- PIN

Process for completing a PCI DSS assessment

Completing a PCI DSS assessment is an in-depth process. The steps required are below:

1. Define the scope of the assessment. This typically involves specifying the technical environment and relevant business units.
2. Using the PCI DSS, do an assessment against all of the testing procedures.

3. Complete the proper report (i.e., Self-*Assessment Questionnaire* (SAQ) or *Report on Compliance* (ROC)) for your company's merchant level (more on that below).
4. Fill out an Attestation of Compliance for Service Providers or Merchants from the PCI SSC website.
5. Submit the SAQ or ROC, and the Attestation of Compliance, to the requestor.
6. If needed, do remediations and submit documentation of those.

PCI Terms

- PAN - Primary Account Number.
- QSA - Qualified Security Assessor.
- CHD - Cardholder Data.
- SAD - Sensitive Authentication Data.
- SAQ - Self Assessment Questionnaire. This is completed by the company.
- ROC - Report on Compliance. These are completed by a QSA (approved assessor) and require an onsite assessment.
- CDE - Cardholder Data Environment
- AOC - Attestation of Compliance.
- ASV - Approved Scan Vendor.

PCI DSS is a security standard that applies to all companies that touch cardholder data, including Merchants and Service Providers that provide technology and services to support Merchant cardholder activities.

About this course

This course is an introduction to PCI. It covers the basics of PCI - types of entities, best practices, and the overall structure of the DSS. Once you’ve completed this course, our PCI-DSS In-Depth course goes into detail about the rules and requirements in the DSS.